КРИПТОСИТЕМЫ С ОТКРЫТЫМ КЛЮЧЕМ, ОСНОВАННЫЕ НА ЛИНЕЙНЫХ КОДАХ НАД НЕКОММУТАТИВНЫМИ АЛГЕБРАМИ[2]

*В.Г. Лабунец**
*Екатеринбург, ФГАОУ ВПО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина», vlabunets05@yahoo.com

PUBLIC KEY CRIPTOSYSTEMS BASED ON LINEAR CODES OVER NONCOMMUTATIVE ALGEBRAS

V.G. Labunets

1. Введение

Популярным классом ассиметричных криптосистем являются системы, основанные на линейных кодах. Впервые такая система была предложенная в [1]. Позже было установлено, что задача декодирования произвольного двоичного линейного кода является NP-полной задачей [2]. Преимуществом таких систем является их высокое быстродействие и возможность исправлять ошибки при доставке шифротекста законному пользователю. Недостаток этих систем – большой объем открытого ключа. Для того, чтобы семейство линейных кодов можно было использовать для построения системы открытого шифрования необходимо, чтобы это семейство удовлетворяло следующим требованиям: 1) семейство содержит достаточно большое число кодов с одинаковыми параметрами с тем, чтобы избежать атаки путем полного перебора всех возможных кодов, 2) каждый код семейства обладает простыми процедурами кодирования и декодирования при условии, что известно полное описание кода, 3) получение полного описания кода из открытого ключа должно представлять собой трудную задачу.

В работе [1] использовано семейство двоичных кодов Гоппы, причем открытым ключом является скремблированная порождающая матрица выбранного кода. Известны несколько более или менее безуспешных атак на эту систему [3,4]. Система Нидерратера [5], основанная на обобщенных кодах Рида-Соломона (ОРС-кодах) использует в качестве открытого ключа скремблированную проверочную матрицу кода. Как показано в [6,7], эта система и некоторые ее варианты могут быть взломаны за полиномиальное время, что является следствием малочисленности семейства ОРС-кодов по сравнению со всем семейством линейных кодов. В этой работе мы предлагаем в существенной мере расширить класс ОРС-кодов за счет использования некоммутативных алгебр Клиффорда $Clif_n\{\mathbf{GF}(p)\}$ над простыми полями Галуа $\mathbf{GF}(p)$ вместо расширенных полей Галуа $\mathbf{GF}(p^n)$.

2. Алгебраическое кодирование над некоммутативными телами

Все до сих пор рассматриваемые ассиметричные криптосистемы используют коды над конечными полями Галуа. Пусть $\mathbf{GF}(q)$ - конечное поле из q элементов, где q степень простого числа p. Рассмотрим N - мерное пространство $\mathbf{V}_N[\mathbf{GF}(q)]=\mathbf{GF}^N(q)$ над полем $\mathbf{GF}(q)$, содержащее q^N векторов $\mathbf{x}=(x_1,x_2,...,x_N)$ длины N с компонентами из $\mathbf{GF}(q)$.

[2] Работа выполнена при финансовой поддержке РФФИ, гранты № 11-07-12017-офи_м и 12-07-12080-офи_м

Пространство $(M\times N)$-матрица над $\mathbf{GF}(q)$ обозначим символом $Mat_{M\times N}\left[\mathbf{GF}(q)\right]=\mathbf{GF}^{M\times N}(q)$. В таком пространстве "живут" проверочные и порождающие матрицы линейных кодов. Класс ОРС-кодов образует маломощное подмножество этого пространства, поэтому криптостойкость ОРС-кодов низка. Ситуация кардинальным образом меняется если вместо коммутативных полей Галуа использовать некоммутативные алгебры Клиффорда.

Пусть $\mathbf{G}^{\boldsymbol{\sigma}}=[w_{ik}^{\sigma_{ik}}]_{i,k=1}^{N}$ - $(N\times N)$-матрица над некоммутативной алгеброй Клиффорда $Clif\left\{\mathbf{GF}(p)\right\}$, каждый матричный элемент $w_{ik}^{\sigma_{ik}}$ которой оснащен меткой σ_{ik}, которая показывает, с какой стороны компонента $w_{ik}^{\sigma_{ik}}$ умножает компоненту x_k вектора $\mathbf{x}=\left(x_1,x_2,...,x_N\right)$,где $x_k\in Clif\left\{\mathbf{GF}(p)\right\}$, при действии $\mathbf{y}^{\boldsymbol{\sigma}}=\mathbf{G}^{\boldsymbol{\sigma}}\mathbf{x}$ $\left(y_i^{\boldsymbol{\sigma}}=\sum_{k=1}^{n}w_{ik}^{\sigma_{ik}}x_k\right)$:

$$w_{ik}^{\sigma_{ik}}x_k=\begin{cases}w_{ik}x_k, & \sigma=1,\\ x_kw_{ik}, & \sigma=0.\end{cases} \tag{1}$$

Все метки σ_{ik} формируют бинарную матрицу $\boldsymbol{\sigma}=\left[\sigma_{ik}\right]$.

Определение 1. Пространство $Mat_{M\times N}^{\boldsymbol{\sigma}}\left[Clif\left\{\mathbf{GF}(p)\right\}\right]$, оснащенное матричной меткой $\boldsymbol{\sigma}=\left[\sigma_{ik}\right]$, назовем пространством с *секретом,отмычкой* или с *потайным ходом* $\boldsymbol{\sigma}=\left[\sigma_{ik}\right]$.

Очевидно, что существует целое семейство $\left\{Mat_{M\times N}^{\boldsymbol{\sigma}}\left[Clif\left\{\mathbf{GF}(p)\right\}\right]\right\}_{\boldsymbol{\sigma}\in\mathbf{B}_2^{M\times N}}$ из $2^{M\times N}$ различных пространств. Для $M=N=16$ это число громадно $2^{16\times16}=2^{256}=64\cdot10^{25}$!

Пусть $\mathbf{G}^{\boldsymbol{\sigma}}=[w_{kj}^{\sigma_{kj}}]_{k,j=1}^{M,N}$ и $\mathbf{H}^{\boldsymbol{\alpha}}=[v_{ik}^{\alpha_{ik}}]_{i,k=1}^{N,M}$ две произвольные матрицы (генерирующая и проверочная) размеров $(M\times N)$ и $(N\times M)$, матричные элементы которых состоят из унимодулярных чисел. Тогда для $\mathbf{y}={}^{2}\mathbf{H}^{\boldsymbol{\alpha}}\cdot{}^{1}\mathbf{G}^{\boldsymbol{\sigma}}\cdot\mathbf{x}$ имеем $y_i=\sum_{j=1}^{N}\left(\sum_{k=1}^{M}{}^{2}v_{ik}^{\alpha_{ik}}\cdot{}^{1}w_{kj}^{\sigma_{kj}}\cdot x_j\right)$, где левые верхние индексы обозначают порядок воздействия матриц на вектор. Произведение ${}^{2}v_{ik}^{\alpha_{ik}}\cdot{}^{1}w_{kj}^{\sigma_{kj}}\cdot x_j$ в зависимости от значений бинарных меток может быть записано в четырех формах

$${}^{2}v_{ik}^{\alpha_{ik}}\cdot{}^{1}w_{kj}^{\alpha_{kj}}\cdot x_j=\begin{cases}{}^{2}v_{ik}\cdot{}^{1}w_{kj}\cdot x_j, & \left(\alpha_{ik}=1\right)\&\left(\sigma_{kj}=1\right),\\ {}^{2}v_{ik}\cdot x_j\cdot{}^{1}w_{kj}, & \left(\alpha_{ik}=1\right)\&\left(\sigma_{kj}=1\right),\\ {}^{1}w_{kj}\cdot x_j\cdot{}^{2}v_{ik}, & \left(\alpha_{ik}=1\right)\&\left(\sigma_{kj}=1\right),\\ x_j\cdot{}^{2}v_{ik}\cdot{}^{1}w_{kj}, & \left(\alpha_{ik}=1\right)\&\left(\sigma_{kj}=1\right),\end{cases} \tag{2}$$

Так как числа по предположению унимодулярные, то $v_{ik}\cdot w_{kj}\cdot x_j$, $v_{ik}\cdot x_j\cdot w_{kj}$, $w_{kj}\cdot x_j\cdot v_{ik}$ и $x_j\cdot v_{ik}\cdot w_{kj}$ суть вращения многомерного числа Клиффорда x_j и четыре вышеприведенных выражения можно записать в векторно-матричной форме

$$v_{ik}^{\alpha_{ik}} \cdot w_{kj}^{\alpha_{kj}} \cdot x_j = \begin{cases} R^l(v_{ik}) \cdot R^l(w_{ik}) \cdot \vec{x}_j, & (\alpha_{ik}=1)\&(\sigma_{kj}=1), \\ R^l(v_{ik}) \cdot R^r(w_{ik}) \cdot \vec{x}_j, & (\alpha_{ik}=1)\&(\sigma_{kj}=1), \\ R^r(v_{ik}) \cdot R^l(w_{ik}) \cdot \vec{x}_j, & (\alpha_{ik}=1)\&(\sigma_{kj}=1), \\ R^l(v_{ik}) \cdot R^r(w_{ik}) \cdot \vec{x}_j, & (\alpha_{ik}=1)\&(\sigma_{kj}=1), \end{cases} \quad (3)$$

где $R^l(w_{ik}), R^r(w_{ik})$ и $R^l(v_{ik}), R^r(v_{ik})$ - левые и правые вращательные представления чисел Клиффорда v_{ik} и w_{ik}. Следовательно, имеем

$$\vec{y}_i = \sum_{j=1}^{N}\left(\sum_{k=1}^{M} R\left(v_{ik}^{\alpha_{ik}}\right) \cdot R\left(w_{kj}^{\sigma_{kj}}\right) \cdot \vec{x}_j\right) = \sum_{j=1}^{N}\left(\sum_{k=1}^{M} R\left(v_{ik}^{\alpha_{ik}}\right) \cdot R\left(w_{kj}^{\sigma_{kj}}\right)\right) \cdot \vec{x}_j, \quad (4)$$

где $\vec{x}_j, \vec{y}_i$ - векторные представления многомерных чисел Клиффорда x_j, y_i. Пара матриц $\mathbf{G}^{\boldsymbol{\sigma}} = [w_{ik}^{\sigma_{ik}}]_{i,k=1}^{N}$ и $\mathbf{H}^{\boldsymbol{\alpha}} = [v_{ik}^{\alpha_{ik}}]_{i,k=1}^{N}$ будет взаимообратной, если выполнится равенство $\sum_{k=1}^{M} R\left(v_{ik}^{\alpha_{ik}}\right) \cdot R\left(w_{kj}^{\sigma_{kj}}\right) = I_{ij}$.

Определение 2. Для каждой фиксированной отмычки $\boldsymbol{\sigma} \in \mathbf{B}_2^{M \times N}$ множество всех векторов $\mathbf{y}^{\boldsymbol{\sigma}} = \mathbf{G}^{\boldsymbol{\sigma}}\mathbf{x}$ назовем линейным кодом с порождающей матрицей $\mathbf{G}^{\boldsymbol{\sigma}}$.

Определение 3. Если $\mathbf{G}^{\boldsymbol{\sigma}}$ является преобразованием Фурье-Клиффорда-Галуа и спектр $\mathbf{y}^{\boldsymbol{\sigma}} = \mathbf{G}^{\boldsymbol{\sigma}}\mathbf{x}$ имеет нулевые компоненты $y_b, y_{b+1}, ..., y_{b+\delta-2}$ для некоторых b, δ, то такой линейный код назывем БЧХ-кодом над алгеброй Клиффорда.

Определение 4. Если $\mathbf{G}^{\boldsymbol{\sigma}}$ является преобразованием Фурье-Клиффорда-Галуа и спектр $\mathbf{y}^{\boldsymbol{\sigma}} = \mathbf{G}^{\boldsymbol{\sigma}}\mathbf{x}$ имеет нулевые компоненты $y_b, y_{b+1}, ..., y_{b+\delta-2}$ для некоторых b, δ, а длина кода равна $p-1$ то такой БЧХ-код назовем кодом Рида -Соломона алгеброй Клиффорда.

Наличие процедур быстрого преобразования Фурье-Клиффорда-Галуа делает введенные коды эффективным средством одновременного избыточного кодирования и шифрования данных.

Литература

1. McEliece R.J. A Public Key Cryptosystem Based on Algebraic Coding Theory // JPL DSN Progress Rep. 42-44, 1978, Jan.-Feb, pp.114-116
2. Berlekamp E.R., McEliece R.J., van Tilborg H.C.A. On inherent intractability of certain coding problems // IEEE Trans. Inf. Theory, 1978, Vol. IT-24, No.4, pp.384-386
3. Heiman R., Shamir A. On the Security of Cryptosystem Based on Linear Error Correcting Codes // Applied Mathematics, Weizmann Institute of Science, Rehovot, Israel, 1987
4. Adams C.M.< Meijer H. Security-Related Comments Regarding McEliece Public Key Cryptosystem. – In: Advances in Cryptology – EUROCRYPT'87
5. Niederreiter H. Knapsack-Type Cryptosystem and Algebraic Coding Theory // Probl. Control and Inform. Theory, 1986, Vol.13, No. 2, pp159-166
6. Сидельников В.М.б Шестаков С.О. О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона // Дискрет. Мат. 1992, т. 3, № 3. с. 57-63
7. Сидельников В.М., Шестаков С.О. О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона // Перспективные средства телекоммуникации и интегрированные системы связи / Под ред. В.В. Зяблова. – М.: 1992, с. 48-61